Frank S. Hedin (SBN 291289)
Hedin LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Attorney for Plaintiffs and the Putative Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ALAN SILVA and ELIZABETH MALATY-UHR, individually and on behalf of all others similarly situated, Plaintiffs, v. YANKA INDUSTRIES, INC. D/B/A MASTERCLASS, Defendant.	Case No. 3:24-cv-05264-JD **THIRD AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Alan Silva ("Plaintiff Silva") and Elizabeth Malaty-Uhr ("Plaintiff Malaty-Uhr"), individually and on behalf of all others similarly situated, make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this action for legal and equitable remedies to redress and put a stop to Defendant Yanka Industries Inc. d/b/a MasterClass's practices of knowingly selling, transmitting, and/or otherwise disclosing, to various third parties,

records containing the personal information of each of their subscribers, along with the detailed information revealing their purchase of a subscription to Defendant's video service (collectively "Personal Viewing Information") in violation of the Video Privacy Protection Act, 18 U.S.C. §2710 et seq. ("VPPA").

2. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its subscribers' personally identifying video subscription purchase information to Meta using a snippet of programming code called the "Meta Pixel," which Defendant chose to install on its masterclass.com website. Defendant also systematically transmitted (and continues to transmit today) its subscribers' personally identifying video viewing information to Google, using another third-party tracking technology known as "Google Analytics" and "Google Tag Manager,"[1] which Defendant chose to integrate and install on its website (hereinafter, "Google Analytics").

3. The information Defendant disclosed (and continues to disclose) to Meta, via the Meta Pixel it installed on its website, includes the subscriber's Facebook ID ("FID") coupled with the fact that the subscriber requested or obtained a subscription to the videos available exclusively on Defendant's website. A subscriber's FID is a unique sequence of numbers linked to the Meta profile belonging to that subscriber. The subscriber's Meta profile, in turn, publicly identifies the subscriber by name (and contains other personally identifying information about the subscriber as well). Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a

[1] Google Developers, About Google Tag Manager, https://developers.google.com/tag-platform/tag-manager (last visited Oct. 2, 2024)

name, as numerous persons may share the same name but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals that a particular person purchased a subscription to Defendant's website (hereinafter, "Personal Viewing Information").

4. The information Defendant disclosed (and continues to disclose) to Google Analytics via the Google Tag Manager it installed on its website includes the specific video title and unique user data sufficient for identification of the subscriber.

5. Defendant disclosed and continues to disclose its subscribers' Personal Viewing Information to Meta and Google without asking for let alone obtaining its subscribers' consent to these practices.

6. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), inter alia, liquidated damages in the amount of $2,500.00 per violation and equitable relief, *see id.* § 2710(c).

7. Accordingly, on behalf of themselves and members of the Classes defined below, Plaintiffs bring this Third Amended Class Action Complaint against Defendant

for intentionally and unlawfully disclosing their Personal Viewing Information to Meta and Google.[2]

PARTIES

I. Plaintiff Silva

8. Plaintiff Silva is, and at all times relevant hereto was, a citizen and resident of Bedford County in Alum Bank, Pennsylvania.

9. Plaintiff Silva is, and at all times relevant hereto was, a user of Meta.

10. Plaintiff Silva is a consumer of the video products and services offered on Defendant's masterclass.com website. He first subscribed to Defendant's website in or about December 2023 and has continuously maintained his subscription since then. Plaintiff Silva became a subscriber to Defendant's website by registering and paying for a subscription via the Google quick sign-up feature, which automatically pulled over his name, email address, payment information, and zip code from his Google account.

11. On multiple occasions during the two years preceding the filing of this action, Plaintiff Silva used his subscription to Defendant's website to request and obtain pre-recorded videos from Defendant on his cellular phone and computer. On each such occasion, Defendant disclosed to Google Plaintiff Silva's hashed email address, unique IP addresses, the device name and type on which he requested and viewed the prerecorded video material, the browser he used to request and watch prerecorded video material, and the specific title of the prerecorded video or materials he purchased (as

[2] This Third Amended Class Action Complaint is filed within twenty-one (21) days of service of the Rule 12(b) motion. Fed. R. Civ. P. (15)(a)(1)(B); *Ramirez v. Cnty. of San Bernardino*, 806 F.3d 1002, 1008 (9th Cir. 2015).

well as the URL where such videos are available for purchase), among other information.

12. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Silva had a Meta account, a Meta profile, and an FID associated with such profile.

13. At all times relevant hereto, including when accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Silva had a Google account associated with his email address, corresponding profile, and unique identifiers associated with such profile.

14. Plaintiff Silva has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta or Google. In fact, Defendant has never even provided Plaintiff Silva with written notice of its practices of disclosing its customers' Personal Viewing Information to third parties such as Meta or Google.

15. Because Defendant disclosed Plaintiff Silva's Personal Viewing Information (including his FID and his purchase of a subscription to Defendant's website) to Meta and his Personal Viewing Information to Google during the applicable statutory period, Defendant violated Plaintiff Silva's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

II. Plaintiff Malaty-Uhr

16. Plaintiff Malaty-Uhr is, and at all times relevant hereto was, a citizen and resident of DuPage County, Illinois.

17. Plaintiff Malaty-Uhr is, and at all times relevant hereto was, a user of Meta.

18. Plaintiff Malaty-Uhr is a consumer of the video products and services offered on Defendant's masterclass.com website. She first subscribed to Defendant's website on or about December 2023 and has continuously maintained her subscription since then. Plaintiff Malaty-Uhr became a subscriber to Defendant's website by registering and paying for a subscription via the Google quick sign-up feature, which automatically pulled over her name, email address, payment information, and zip code from her Google account.

19. On multiple occasions during the two years preceding the filing of this action, Plaintiff Malaty-Uhr used her subscription to Defendant's website to request and obtain pre-recorded videos from Defendant on her cellular phone and computer. On each such occasion, Defendant disclosed to Google Plaintiff Malaty-Uhr's hashed email address, unique IP addresses, the device name and type on which she requested and viewed the prerecorded video material, the browser she used to request and watch prerecorded video material, and the specific title of the prerecorded video or materials she purchased (as well as the URL where such videos are available for purchase), among other information.

20. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material

provided to subscribers on Defendant's website, Plaintiff Malaty-Uhr had a Meta account, a Meta profile, and an FID associated with such profile.

21. At all times relevant hereto, including when accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Malaty-Uhr had a Google account associated with her email address, corresponding profile, and unique identifiers associated with such profile.

22. Plaintiff Malaty-Uhr has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Personal Viewing Information to Meta or Google. In fact, Defendant has never even provided Plaintiff Malaty-Uhr with written notice of its practices of disclosing its customers' Personal Viewing Information to third parties such as Meta or Google.

23. Because Defendant disclosed Plaintiff Malaty-Uhr's Personal Viewing Information (including her FID and her purchase of a subscription to Defendant's website) to Meta and her Personal Viewing Information to Google during the applicable statutory period, Defendant violated Plaintiff Malaty-Uhr's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

Defendant Yanka Industries Inc. d/b/a MasterClass

25. Defendant is a Delaware Foreign Business Corporation with its headquarters and principal place of business located at 660 4th Street, San Francisco, CA 94107.

26. Defendant operates and maintains the website masterclass.com, where it sells subscriptions to consumers to access prerecorded video content and provides its

subscribers with access to a digital library comprised of various types of pre-recorded instructional and educational videos.

JURISDICTION AND VENUE

27. This Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

28. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in San Francisco, CA, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

29. Generally speaking, the VPPA prohibits companies like Defendant from knowingly disclosing to third parties like Facebook information that personally identifies consumers like Plaintiffs as having viewed particular videos or other audio-visual products or services.

30. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business…of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4), and defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3)

31. The VPPA's purpose is as apropos today as it was at the time of its enactment over 35 years ago. Leading up to the statute's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials, because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

32. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, it is the personal nature of such information, and the need to protect it from disclosure, that is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

33. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more

pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[3]

34. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[4]

35. In this case, however, Defendant deprived Plaintiffs and the unnamed Class members of that right by systematically (and surreptitiously) disclosing their Personal Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

36. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of

[3] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

[4] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, frank.senate.gov (Jan. 31, 2012).

collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[5]

37. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a $26 billion dollar per year online advertising industry in the United States.[6]

38. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[7]

39. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[8]

---

[5] FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[6] *See Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[7] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[8] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/.

40. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[9]

41. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[10]

42. Recognizing the serious threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[11]

---

[9] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of- consumer-database-marketing.html.

[10] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c.

[11] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

43. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendant share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[12]

44. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[13] The FTC notes that "[t]she elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[14]

45. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like

---

[12] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[13] *Id.*

[14] *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared statement of the FTC), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[15]

46. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices When Making Purchases

47. As the data aggregation industry has grown, so too have consumer concerns regarding their personal information.

48. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do not protect their privacy online.[16] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[17]

---

[15] *Id.*

[16] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[17] *Id.*

49. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy- protective competitors.

50. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[18]

51. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[19]

52. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[20] As such,

---

[18] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), *available at* http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[19] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on monetising privacy* (Feb. 27, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

[20] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf ("It is obvious that people value online privacy.").

where a business offers customers a service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a service of less value than the service paid for.

III. Defendant Systematically Discloses its Subscribers' Personal Viewing Information to Third Parties

53. As alleged below, when a consumer requests or obtains a specific subscription to Defendant's website, the Meta Pixel technology that Defendant intentionally installed on its website transmits the fact that a consumer purchased a subscription to video services alongside his or her FID to Meta, without the subscriber's consent and in clear violation of the VPPA.

54. Also, when a subscriber to Defendant's website requests or obtains a specific video, Defendant discloses to Google Analytics, through the operation of Google Analytics, the user's (i) hashed email address, (ii) Google Analytics client ID ("cid"), (iii) the title, unique numerical identifier, and URL of the video the user is watching, and (iv) excessive amounts of other uniquely identifiable data points, or predefined user dimensions, just short of a person's name that include: age, browser type, city, continent and subcontinent, country, device brand, gender, interests, language, operating system, OS version, IP address, platform, region.[21] This information is disclosed to Google Analytics without the subscriber's consent and in clear violation of the VPPA.

A. The Meta Pixel

55. On February 4, 2004, Mark Zuckerberg and others launched Facebook,

[21] Google Analytics Help, *Dimensions and metrics [GA4] Predefined user dimensions signals*, https://support.google.com/analytics/answer/9268042?visit_id=638630753515343005-1876215053&rd=2 (last visited Sept. 28, 2024).

now known as "Meta".[22] Since then, Meta has become the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birthdate, gender, and phone number or email.

56. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to allow them to track consumers' actions and report the actions back to Meta.

57. The Meta Pixel allows online-based companies like Defendant to build detailed profiles about their visitors by collecting information about how they interact with their websites, and to then use the collected information to service highly targeted advertising to them.

58. Additionally, a Meta Pixel installed on a company's website allows Meta "to match . . . website visitors to their respective [Meta] User accounts."[23] Meta is able to do this because it has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[24] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after clearing browser history.

---

[22] Company Info, FACEBOOK, https://about.fb.com/company-info./.

[23] https://developers.facebook.com/docs/meta-pixel/get-started.

[24] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

59. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

60. Simply put: if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to "track[] the people and type of actions they take"[25] on the company's website, including the purchases they made, the items they spent time viewing, and, as relevant here, the specific video content that they requested or obtained on the website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Personal Viewing Information of all of its Subscribers to Meta

61. Defendant allows persons to become digital consumers of its various online-based video products and services by subscribing to its website. To subscribe, the consumer must provide at least his or her name, email address, billing address, and credit- or debit-card (or other form of payment) information.

62. When a person is completing the subscription process to gain access to videos on Defendant's website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the subscriber and

[25] https://www.facebook.com/business/goals/retargeting.

the fact that the person is requesting or obtaining a subscription to Defendant's website.

63. Defendant intentionally programmed its website (by following step-by-step instructions from Meta's website) to include a Meta Pixel that systematically transmits to Meta the FIDs of its subscribers and the fact that a subscription was purchased by each of them in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

64. With only a person's FID and the knowledge that a person purchased a subscription to Defendant's website—all of which Defendant knowingly provides to Meta —any ordinary person could learn the identity of the person to whom the FID corresponds and the specific video products or services that this person requested. This can be accomplished simply by accessing the URL www.facebook.com/[unencrypted FID]/.

65. Defendant's practices of disclosing that Plaintiffs and members of the Classes purchased subscriptions on Defendant's website to Meta continued unabated for the full duration of the time period relevant to this action. At all times relevant hereto, whenever Plaintiffs or another subscriber of Defendant's website requested or obtained a particular subscription (by clicking on it) on Defendant's website, Defendant disclosed to Meta that (*inter alia*) the purchaser requested or obtained a subscription to video services, along with the FID of the subscriber who requested it (which, as discussed above, uniquely identifies the person).

66. At all relevant times, Defendant knew the Meta Pixel disclosed its subscribers' Personal Viewing Information to Meta.

67. Defendant could easily have programmed its website so that none of its

subscribers' detailed Personal Viewing Information is disclosed to Meta. Instead, Defendant chose to program its website so that all of its subscribers' detailed Personal Viewing Information is sent to Meta *en masse*.

C. Google Analytics

68. Google Analytics functions like the Meta Pixel, in that, when a subscriber to Defendant's website requests or obtains a specific video, Google Analytics – as intentionally installed on Defendant's website – transmits or collects unique information sufficient for identification of the user including by their hashed email or IP Addresses and other detailed information concerning the specific interactions the subscriber takes on its website (including the subscriber's Personal Viewing Information revealing the specific videos that he or she requested), without the subscriber's consent and in clear violation of the VPPA.

69. When a subscriber to Defendant's website requests or obtains a particular prerecorded video by clicking on it, the title of the prerecorded video content and the prerecorded video content's product number are transmitted to Google Analytics alongside the subscriber's client id ("cid"),[26] hashed email address, NID,[27] IP address,

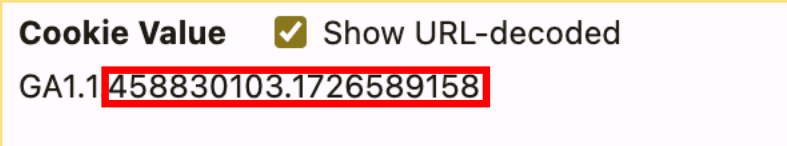
[26] Google Analytics *Help, [GA4] Data collection*, https://support.google.com/analytics/answer/11593727?hl=en (last visited Sept. 28, 2024) ("Google Analytics stores a client ID in a first-party cookie named _ga to distinguish unique users and their sessions on your website.").

[27] Defendant even discloses a unique identifier to Google Analytics for each subscriber who is not signed into their Google account at the time they request or obtain videos from Defendant's website, and that identifier is the NID which directly relates back to one's Google account. *See* Google, *How Google uses cookies*, https://policies.google.com/technologies/cookies (last visited Sept. 28, 2024) ("The 'NID' cookie is used to show Google ads in Google services for *signed-out users*") (emphasis added).

and unique device identifiers. This information can be used by an ordinary person to identify the specific subscriber.

70. Specifically, each subscriber to Defendant's website is assigned a "cid" by Defendant and its use of Google Analytics to distinguish between individual users and their sessions on Defendant's website.

71. A subscriber's cid and unique id "uid" are also communicated through cookies within that same Google Analytics code. The cookie values are displayed in the developer settings of the browser and reveal the particular cid within the _ga cookie, as seen in the following exemplar:



72. This _ga cookie is comprised of four parts separated by periods: (1) a version number "GA[#]", (2) the number of components at the domain, (3) a unique ID # for the user, and (4) a timestamp of the user's first visit to the site. The last two parts collectively make up the client id.

73. An email address is a personally identifying string of characters that designate an electronic mailbox. Any ordinary person can use an e-mail address to uniquely identify the individual to whom it belongs. Voluminous services exist which enable individuals to look up the owners of a particular email address.

74. A "hash" is an algorithm used to create a digital summary, or fingerprint, of the input. However, the Federal Trade Commission has warned companies for over a decade that hashing is an insufficient method of anonymizing information, including

as recently as July 24, 2024.[28] Thus, even in hashed form, email addresses are traceable to individuals.

75. The IP addresses transmitted by Defendant to Google Analytics create an approximate map to follow the subscriber across devices and locations. This is because the IP address changes depending on the subscriber's location and device. In the case of Plaintiffs, each time they viewed a particular video from Defendant's website, Defendant disclosed their personal IP addresses corresponding to the mobile device or computer used. If Plaintiffs used a different device from a different location, Google Analytics received a different IP address, and each IP address remained associated with the individual Plaintiff's masterclass.com account, client ID, hashed email address, and other unique device identifiers disclosed to Google Analytics.

76. In sum, as an example of the information disclosed by Defendant to Google Analytics, the information would reveal that a 34-year-old woman from Charlotte, North Carolina (North America - USA), with unique hashed email address - x, corresponding client ID, home IP Address of 69.217.130.96, using Mozilla Firefox on a MacOsX Sierra Studio computer, requested or obtained a specific video product from www.masterclass.com.

77. Simply put, when a person requests or obtains prerecorded video from

[28] Ed Felten, *Does Hashing Make Data "Anonymous"?*, Federal Trade Commission (Apr. 22, 2012), available at https://www.ftc.gov/policy/advocacy-research/tech-atftc/2012/04/does-hashing-make-data-anonymous; Federal Trade Commission, *No, Hashing Still Doesn't Making Your Data Anonymous* (July 24, 2024), available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

Defendant's website, Google Analytics or any ordinary person can identify that user by email address, client ID, or by using the approximate map of IP addresses when coupled with the other identifiers discussed above.

78. Prior to transmitting its subscribers' Personal Viewing Information to Meta or Google Analytics, Defendant failed to notify Plaintiffs or any of its other subscribers that it would do so, and neither Plaintiffs nor any of its other subscribers have consented (in writing or otherwise) to these practices.

79. By intentionally disclosing to Meta and Google Analytics Plaintiffs' and its other subscribers' FIDs and other identifiers together with the specific video content they each requested or obtained, without Plaintiffs' or any of its other subscribers' consent to these practices, Defendant knowingly and systematically violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

80. Plaintiffs seek to represent two classes defined as follows:

> **Meta Class**: All persons in the United States who, during the two years preceding the filing of this action, requested or obtained a subscription to Defendant's website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.
>
> **Google Class**: All persons in the United States who, during the two years preceding the filing of this action, requested or obtained video content as a subscriber of Defendant's website while maintaining an account with Google.

81. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Classes number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Members

of the Classes may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

82. Common questions of law and fact exist for members of all Classes and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to: (a) whether Defendant knowingly disclosed Plaintiffs' and Class members' Personal Viewing Information to third parties; (b) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiffs' and Class members' Personal Viewing Information to Meta; (d) whether Defendant should be enjoined from disclosing Plaintiffs' and Class members' Personal Viewing Information to Google; and (e) whether Plaintiffs and Class members are entitled to statutory damages for the aforementioned violations.

83. The named Plaintiffs' claims are typical of the claims of the Classes in that the named Plaintiffs and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Personal Viewing Information to Meta and Google.

84. Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the Class members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of members of the Classes.

85. The class mechanism is superior to other available means for the fair and efficient adjudication of Classes claims. Each individual member of the Classes may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT ONE
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710
Meta Class

86. Plaintiffs repeat the allegations from paragraphs (1-51, 53-65, 67-74) as if fully set forth herein.

87. Plaintiffs bring this claim individually and on behalf of the Meta Class Members against Defendant.

88. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

89. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

90. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and the Meta Class members are consumers because they purchased a subscription to prerecorded video content on Defendant's website. Thus, Plaintiffs and the Meta Class members are "consumers" as defined in 18 U.S.C. § 2710(a)(1).

91. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Defendant knowingly disclosed Plaintiffs' and the Meta Class members' Personal Viewing Information to Meta in the manner alleged herein. The Personal Viewing Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because the transmitted information identified Plaintiffs and each Meta Class member to Meta as an individual who purchased a subscription to video content from Defendant's website.

92. Defendant never obtained informed, written consent from Plaintiffs or any Meta Class member to disclose their Personal Viewing Information to Meta or any other

third party. More specifically, Defendant never obtained from Plaintiffs or any Meta Class member's informed, written consent in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; Defendant never obtained from Plaintiffs or any Meta Class member's informed, written consent that, at the election of the consumer, was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and conspicuous manner, for Plaintiffs or any Meta Class member to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

93. Defendant knowingly disclosed such information to Meta because Defendant intentionally installed and programmed the Meta Pixel code on its website, knowing that such code would transmit to Meta the subscription purchased by its consumers and the purchasers' unique identifiers (including FIDs).

94. By disclosing Plaintiffs' and Meta Class members' Personal Viewing Information, Defendant violated their statutorily protected right to privacy in the video services they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

95. As a result of these violations, Defendant is liable to Plaintiffs and Meta Class members for damages and other relief as provided by the VPPA.

96. On behalf of themselves and all members of the Meta Class, Plaintiffs seek to enjoin Defendant's future disclosures of its purchasers' Personal Viewing Information; liquidated damages in the amount of $2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the

Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

COUNT TWO
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710
Google Class

97. Plaintiffs repeat the allegations from paragraphs (1-74) as if fully set forth herein.

98. Plaintiffs bring this claim individually and on behalf of the Google Class Members against Defendant.

99. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

100. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

101. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and Google Class members are subscribers to Defendant's prerecorded video content service. Thus, Plaintiffs and the Google Class members are "consumers" as defined in 18 U.S.C. § 2710(a)(1).

102. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information'

includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Defendant knowingly disclosed Plaintiffs' and the Google Class members' Personal Viewing Information to Google in the manner alleged herein. The Personal Viewing Information that Defendant transmitted to Google constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because Google is an email service and electronic communication service provider akin to an ISP that stores IP addresses alongside other user information (name, email, phone number) and the information transmitted by Defendant informed Google of (1) Plaintiffs' and class members' IP addresses during each visit on different devices that directly link back to their masterclass.com and Gmail accounts, (2) Plaintiffs' and class members' hashed email addresses, (3) other information sufficient to identify Plaintiffs, and each Google Class member, and (4) the specific video materials requested or obtained from Defendant's website.

103. Defendant never obtained informed, written consent from Plaintiffs or any Google Class member to disclose their Personal Viewing Information to Google or any other third party. More specifically, Defendant never obtained from Plaintiffs or any Google Class member's informed, written consent in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer. Defendant never obtained from Plaintiffs or any Google Class member's informed, written consent that, at the election of the consumer, was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and conspicuous manner, for Plaintiffs or any Google Class

member to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

104. Defendant knowingly disclosed such information to Google because Defendant intentionally installed and programmed the Google Analytics code on its website, knowing that such code would transmit to Google or allow Google to simultaneously collect the specific video titles requested or obtained on Defendant's website, the user's IP address, and other information sufficient for Google to identify the particular subscriber.

105. By disclosing Plaintiffs' and Google Class members' Personal Viewing Information, Defendant violated their statutorily protected right to privacy in the videos they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

106. As a result of these violations, Defendant is liable to Plaintiffs and Google Class members for damages and other relief as provided by the VPPA.

107. On behalf of themselves and all members of the Google Class, Plaintiffs seek to enjoin Defendant's future disclosures of its purchasers' Personal Viewing Information; liquidated damages in the amount of $2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek a judgment against Defendant Yanka Industries Inc. d/b/a MasterClass as follows:

A. For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Classes and Plaintiffs' attorneys as Class Counsel to represent the Classes;

B. For an order declaring that Defendant's conduct as described herein violated the VPPA;

C. For an order finding in favor of Plaintiffs and the Classes and against Defendant on all counts asserted herein;

D. For an award of $2,500.00 to the Plaintiffs and members of the Classes, as provided by the VPPA, 18 U.S.C. § 2710(c);

E. For an order permanently enjoining Defendant from disclosing the Personal Viewing Information of its subscribers to third parties in violation of the VPPA.

F. For prejudgment interest on all amounts awarded; and

G. For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiffs and the Classes under Rule 23 and 18 U.S.C. § 2710(c).

JURY DEMAND

Plaintiffs demand a trial by jury on all causes of action and issues so triable.

Dated: November 29, 2024

Respectfully submitted,

/s/ Frank S. Hedin

HEDIN LLP
FRANK S. HEDIN
535 Mission Street, 14th Floor
San Francisco, CA 94105
TELEPHONE: (305) 357-2107
FACSIMILE: (305) 200-8801
FHEDIN@HEDINLLP.COM

Attorney for Plaintiffs and Putative Classes